**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | |
|---|---|
| Applicant: Teng Pin Poo et al. | Group Art Unit: 2133 |
| Serial No.: 09/898,365 | Examiner: Shewaye Gelagay |
| Filed: July 3, 2001 | Confirmation No.: 4356 |
| Title: Portable Device Having Biometrics-Based Authentication Capabilities | Docket No.: 1601457-0007 |

Certificate of Transmission

I hereby certify that this paper is being transmitted to the U.S. Patent and Trademark Office via the Electronic Filing System in accordance with 37 C.F.R. § 1.6(a)(4) on the date indicated below.

Date: 4/23/08 By: Gail Ohlsson
Gail A. Ohlsson

**RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Notification of Non-Compliant Appeal Brief mailed March 28, 2008, Appellants are enclosing a revised "Summary of Claimed Subject Matter" section of the appeal brief filed on March 20, 2008, beginning on page 2 of this paper. The revised section contains a concise explanation of the subject matter of each of the independent claims involved in the appeal (1, 7, 17, and 23), referring to the specification and to the drawings.

## SUMMARY OF CLAIMED SUBJECT MATTER

### Independent Claims 1, 7, and 23

Appellant's invention is directed to a portable data storage device having biometrics-based authentication capabilities so the device can authenticate users before granting access to the data storage capabilities of the device. As illustrated in Figure 1B and Figure 2 of the application, reproduced below, portable device 170 has a housing, within which is housed a microprocessor 111, a biometrics-based authentication module 150 controlled by the microprocessor 111, a non-volatile memory 117, a memory controller 133, and a biometrics sensor 152. Portable device may also have volatile memory 116. *See* Specification page 8, lines 23-27; page 9, lines 7-8 and 15-18. Portable device 170 also includes a USB device controller 115 and a USB plug 118 that is integrated into its housing and which is directly coupled to a USB host controller 193 of a host platform. *See* Specification page 8, lines 2-5.

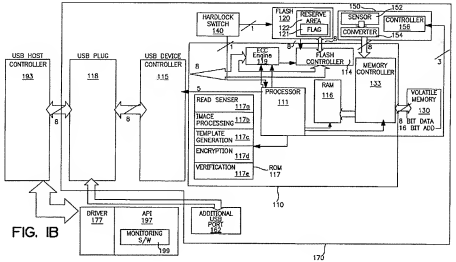


FIG. IB

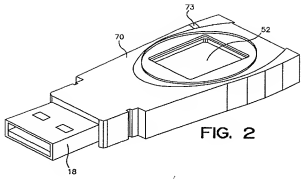


FIG. 2

**Appellants' Patent Application, Figures 1B and 2**

Portable device 170 is used to implement a biometrics-based authentication for controlling access to user data stored on the device. Non-volatile memory 117 stores firmware such as firmware 117a for reading fingerprint sensor 152, firmware 117b for processing fingerprint images, firmware 117c for generating templates, firmware 117d for encrypting fingerprint images and/or templates, and firmware 117e for verifying fingerprint authenticity. *See* Specification page 8, lines 30-33. Upon its first use, portable device 170 guides the user through the registration process wherein the user places his or her finger on fingerprint sensor 152, located on the surface of portable device 170, and sensor 152 is read to capture an acceptable image of the fingerprint. *See* Specification page 12, lines 1-10. An encrypted template is generated based on the fingerprint image and stored into non-volatile memory 117. *See* Specification page 12, lines 13-17. During the authentication process, another image of the user's fingerprint is taken when the user places his or her finger on sensor 152. *See* Specification page 12, lines 32 through page 13, line 1. Microprocessor 111 directs the retrieval of the registered fingerprint template from non-volatile memory 117. *See* Specification page 13, lines 9-10. Next, verification module 117e compares the recently taken fingerprint image against the registered image. *See* Specification page 13, lines 15-17. If a match is detected, and in situations where the portable device is used as a secure storage device, the user is

authenticated and granted access to the portable device. *See* Specification page 14, lines 6-10. If no match is detected, such access is denied. *See* Specification page 13, lines 22-23.

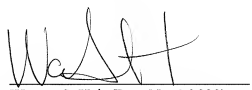
**Independent Claim 17**

Appellants' invention is directed to a biometrics-based authentication method implemented using a portable device 70. A first biometrics marker, such as a fingerprint, is obtained from a user with a biometrics sensor 52 installed on the portable device 70. *See* Specification page 12, line 32 – page 13, line 1; FIG. 10, step 230. Then a registered biometrics marker is retrieved from a flash memory 20 of the portable device 70. *See* Specification page 13, lines 7-10; FIG. 10, step 240. The registered biometrics marker was previously stored in the flash memory 20 during a registration process. *See* Specification page 12, lines 1-31; FIG. 10, steps 225-255. The first biometrics marker is compared to the registered biometrics marker, and the user's access to the non-volatile memory is denied if the first biometrics marker does not match the registered biometrics marker. *See* Specification page 13, lines 14-17; FIG. 10, step 260. If the first biometrics marker matches the registered biometrics marker, an authentication success is signaled. *See* Specification page 13, lines 14-17, FIG. 10, steps 260 and 280.

Respectfully submitted,

WHITE & CASE LLP

Dated: April 13, 2008

By: 

Warren S. Heit (Reg. No. 36,828)
WHITE & CASE LLP
1155 Avenue of the Americas
New York, NY 10036
(650) 213-0321